

# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2.1**

**June 2018**

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

#### Part 1. Service Provider and Qualified Security Assessor Information

##### Part 1a. Service Provider Organization Information

|                   |   |          |                          |                               |        |  |
|-------------------|---|----------|--------------------------|-------------------------------|--------|--|
| Company Name:     | Payment Guide                                       |          | DBA (doing business as): |                               |        |  |
| Contact Name:     | Eugene Chertikhin                                   |          | Title:                   | General manager               |        |  |
| Telephone:        | +7 495 298-7007                                     |          | E-mail:                  | e.chertikhin@payment-guide.ru |        |  |
| Business Address: | office 506, 5 fllor, 16 build 4, Sushevsky val str. |          | City:                    | Moscow                        |        |  |
| State/Province:   | Moscow  | Country: | Russia                   | Zip:                          | 127018 |  |
| URL:              | https://www.payment-guide.ru                        |          |                          |                               |        |  |

##### Part 1b. Qualified Security Assessor Company Information (if applicable)

|                        |   |          |                            |      |        |
|------------------------|---|----------|----------------------------|------|--------|
| Company Name:          | Compliance Control Ltd.                 |          |                            |      |        |
| Lead QSA Contact Name: | Ivan Tverdokhlebov                      | Title:   | Chief Executive Officer    |      |        |
| Telephone:             | +7 926 576 7095                         | E-mail:  | ivan@compliance-control.ru |      |        |
| Business Address:      | Revolutionnaya street blg 3, office 306 | City:    | Volokolamsk                |      |        |
| State/Province:        | Moscow                                  | Country: | Russia                     | Zip: | 143600 |
| URL:                   | http://www.compliance-control.ru        |          |                            |      |        |



## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) assessed: POS-processing (payment gateway) and e-commerce

Type of service(s) assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

#### Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☒ POS / card present
- ☒ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ Account Management

☐ Fraud and Chargeback

☒ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☒ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify):

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.



### Part 2a. Scope Verification (continued)

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) not assessed: N/A

Type of service(s) not assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

#### Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☐ POS / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ Account Management

☐ Back-Office Services

☐ Billing Management

☐ Clearing and Settlement

☐ Network Provider

☐ Fraud and Chargeback

☐ Issuer Processing

☐ Loyalty Programs

☐ Merchant Services

☐ Payment Gateway/Switch

☐ Prepaid Services

☐ Records Management

☐ Tax/Government Payments

☐ Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

### Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Current transaction amount for CNP and CP operations is:

VISA – 1,600,000 annually.

MasterCard – 2,000,000 annually

MIR – 1,850,000 annually

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

No other way of being involved into the ability to impact security of CHD exists except the above.

### Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

| Type of facility:       | Number of facilities of this type | Location(s) of facility (city, country): |
|-------------------------|-----------------------------------|--|
| Example: Retail outlets | 3                                 | Boston, MA, USA                          |
| Office                  | 1                                 | Moscow, Russia                           |
| Datacenter              | 1                                 | Saint-Petersburg, Russia                 |



## Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☒ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

| Payment Application Name | Version Number | Application Vendor     | Is application PA-DSS Listed?                                       | PA-DSS Listing Expiry date (if applicable) |
|--------------------------|----------------|------------------------|---|--|
| Payment Gateway          | 4.0.7          | CrestWave Technologies | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | 28 Oct 2022                                |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |
|                          |                |                        | <input type="checkbox"/> Yes <input type="checkbox"/> No            |  |

## Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- Connections into and out of the cardholder data environment (CDE).
- Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.

The CDE is located in 2 Datacenters with replication and load balancing. Several VLANs with strict segmentation rules are used inside the CDE to limit and control access. External connections are available only for host-2-host connections with Banks and for POS-terminals connections.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

☒ Yes ☐ No

## Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?

☐ Yes ☒ No

**If Yes:**

Name of QIR Company:

N/A

QIR Individual Name:

N/A

Description of services provided by QIR:

N/A

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

☐ Yes ☒ No

**If Yes:**

Name of service provider:

Description of services provided:

|  |  |
|--|--|
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Note:** Requirement 12.8 applies to all entities in this list.



## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

| <b>Name of Service Assessed:</b> |                                     | ACS Hosting provider and ATM/POS-processing |                          |   |
|----------------------------------|-------------------------------------|---|--------------------------|---|
| PCI DSS Requirement              | Details of Requirements Assessed    |   |                          | Justification for Approach<br>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)        |
|                                  | Full                                | Partial                                     | None                     |   |
| Requirement 1:                   | <input type="checkbox"/>            | <input checked="" type="checkbox"/>         | <input type="checkbox"/> | 1.2.3 - Wireless networks are not used within CDE.  |
| Requirement 2:                   | <input type="checkbox"/>            | <input checked="" type="checkbox"/>         | <input type="checkbox"/> | 2.1.1 - Wireless networks are not used within CDE.<br>2.6 - The entity is not a shared hosting provider.  |
| Requirement 3:                   | <input type="checkbox"/>            | <input checked="" type="checkbox"/>         | <input type="checkbox"/> | 3.4.1 - Full-disk encryption is not used.   |
| Requirement 4:                   | <input type="checkbox"/>            | <input checked="" type="checkbox"/>         | <input type="checkbox"/> | 4.1.1 - Wireless networks are not used within CDE<br>4.2 - PANs are not sent via end-user message services.   |
| Requirement 5:                   | <input checked="" type="checkbox"/> | <input type="checkbox"/>                    | <input type="checkbox"/> |   |
| Requirement 6:                   | <input checked="" type="checkbox"/> | <input type="checkbox"/>                    | <input type="checkbox"/> |   |
| Requirement 7:                   | <input checked="" type="checkbox"/> | <input type="checkbox"/>                    | <input type="checkbox"/> |   |
| Requirement 8:                   | <input type="checkbox"/>            | <input checked="" type="checkbox"/>         | <input type="checkbox"/> | 8.1.5 - No external vendors connections are used.<br>8.5.1 - No remote access to customers is used.   |
| Requirement 9:                   | <input type="checkbox"/>            | <input checked="" type="checkbox"/>         | <input type="checkbox"/> | 9.6.2, 9.6.3 - No media with CHD are sent outside the facility.<br>9.7.1, 9.8.1 - There is not any kind of media (paper or removable electronic media). |
| Requirement 10:                  | <input checked="" type="checkbox"/> | <input type="checkbox"/>                    | <input type="checkbox"/> |   |
| Requirement 11:                  | <input checked="" type="checkbox"/> | <input type="checkbox"/>                    | <input type="checkbox"/> |   |

|                 |                                     |                          |                                     |  |
|-----------------|-------------------------------------|--------------------------|-------------------------------------|--|
| Requirement 12: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |  |
| Appendix A1:    | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | The entity is not a shared hosting provider. |
| Appendix A2:    | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Unsecure protocols are not used.             |



## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

|  |   |  |
|--|---|--|
| The assessment documented in this attestation and in the ROC was completed on: | June 10, 2021                           |  |
| Have compensating controls been used to meet any requirement in the ROC?       | <input type="checkbox"/> Yes            | <input checked="" type="checkbox"/> No |
| Were any requirements in the ROC identified as being not applicable (N/A)?     | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No            |
| Were any requirements not tested?  | <input type="checkbox"/> Yes            | <input checked="" type="checkbox"/> No |
| Were any requirements in the ROC unable to be met due to a legal constraint?   | <input type="checkbox"/> Yes            | <input checked="" type="checkbox"/> No |

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated June 10, 2021.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (*check one*):

☒ **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby **Payment Guide** has demonstrated full compliance with the PCI DSS.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby (*Service Provider Company Name*) has not demonstrated full compliance with the PCI DSS.

**Target Date** for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*

☐ **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

*If checked, complete the following:*

| Affected Requirement | Details of how legal constraint prevents requirement being met |
|----------------------|--|
|                      |  |
|                      |  |

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(*Check all that apply*)

- ☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
- ☒ All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
- ☒ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- ☒ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- ☒ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.



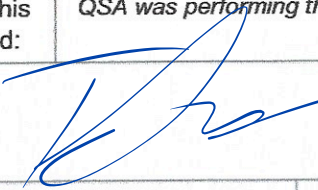
**Part 3a. Acknowledgement of Status (continued)**

|                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment. |
| <input checked="" type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor <b>Clone Systems, Inc.</b>   |

**Part 3b. Service Provider Attestation**

|   |                               |
|---|-------------------------------|
|  |                               |
| Signature of Service Provider Executive Officer ↑                                 | Date: <b>June 10, 2021</b>    |
| Service Provider Executive Officer Name: <b>Eugene Chertikhin</b>                 | Title: <b>General Manager</b> |

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

|  |   |
|--|---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | QSA was performing the assessment.          |
|    |   |
| Signature of Duly Authorized Officer of QSA Company ↑                                | Date: <b>June 10, 2021</b>                  |
| Duly Authorized Officer Name: <b>Ivan Tverdokhlebov</b>                              | QSA Company: <b>Compliance Control Ltd.</b> |

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

|   |     |
|---|-----|
| If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed: | N/A |
|---|-----|

- <sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.
- <sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.
- <sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

| PCI DSS Requirement | Description of Requirement   | Compliant to PCI DSS Requirements<br>(Select One) |                          | Remediation Date and Actions<br>(If "NO" selected for any Requirement) |
|---------------------|--|---|--------------------------|--|
|                     |  | YES   | NO                       |  |
| 1                   | Install and maintain a firewall configuration to protect cardholder data                                       | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 2                   | Do not use vendor-supplied defaults for system passwords and other security parameters                         | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 3                   | Protect stored cardholder data   | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 4                   | Encrypt transmission of cardholder data across open, public networks   | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 5                   | Protect all systems against malware and regularly update anti-virus software or programs                       | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 6                   | Develop and maintain secure systems and applications   | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 7                   | Restrict access to cardholder data by business need to know  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 8                   | Identify and authenticate access to system components  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 9                   | Restrict physical access to cardholder data  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 10                  | Track and monitor all access to network resources and cardholder data  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 11                  | Regularly test security systems and processes  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 12                  | Maintain a policy that addresses information security for all personnel  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| Appendix A1         | Additional PCI DSS Requirements for Shared Hosting Providers   | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| Appendix A2         | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |

